

**G.I., individually and on behalf of all
others similarly situated,**

Plaintiffs,

V.

DAVITA, INC.,
Serve Registered Agent:
Corporation Service Company
1900 W Littleton Blvd.
Littleton, CO 80120

Defendant.

Case No:

Division:

CLASS ACTION PETITION FOR DAMAGES

COMES NOW (“Plaintiff”), individually and on behalf of all citizens who are similarly situated for her Class Action Petition for Damages against Defendant DaVita, Inc. (hereinafter sometimes referred to as “Defendant DaVita” and/or “DaVita”), respectfully states and alleges as follows:

NATURE OF THE CASE

1. This is a class action brought by Plaintiff, individually and on behalf of all citizens who are similarly situated (*i.e.*, the Class Members), seeking to redress Defendant’s willful and reckless violations of her privacy rights. Plaintiff and the other Class Members are patients of DaVita who entrusted their personal health information (“PHI”) and personally identifiable information (“PII”) to DaVita. Defendant DaVita has shared Plaintiff’s PHI and PII with persons who are not authorized to have said PHI and PII. Defendant betrayed Plaintiff’s and the Class Members’ trust by failing to properly safeguard and protect their PHI and PII and publicly disclosing their PHI and PII without authorization in violation of Missouri common law.

2. This action pertains to Defendant's unauthorized disclosure of the Plaintiff's PHI and PII that occurred on or around April 12, 2025 (the "Breach").¹

3. Defendant disclosed Plaintiff's and the other Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendant's failure to safeguard and protect their PHI and PII.

4. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and the other Class Members' patient information.²

5. Defendant flagrantly disregarded Plaintiff's and the other Class Members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PHI and PII from unauthorized disclosure. Plaintiff's and the other Class Members' PHI and PII was improperly handled, inadequately protected, readily able to be copied by thieves and not kept in accordance with basic security protocols. Defendant's obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and the other Class Members' rights, both as to privacy and property.

6. Plaintiff has standing to bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the additional damages set forth in detail below, which are incorporated herein by reference.

7. Defendant's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research

¹ <https://www.hipaajournal.com/davita-ransomware-attack/> (Last visited on April 30, 2025).

² *Id.*

(“Javelin”), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report (“the Javelin Report”), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PHI and PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff’s and the other Class Members’ PHI and PII and not yet used the information will do so at a later date or re-sell it.

8. Plaintiff and the Class Members have also suffered and are entitled to damages for the lost benefit of their bargain with Defendant DaVita. Plaintiff and members of the Class paid DaVita for its services including them protecting their PHI and PII. The lost benefit of the bargain is measured by the difference between the value of what Plaintiff and the members of the Class should have received when they paid for their services, and the value of what they actually did receive; services without adequate privacy safeguards. Plaintiff and members of the Class have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiff and the members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

9. Additionally, because of Defendant’s conduct, Plaintiff and members of the Class have been harmed in that Defendant has breached its common law fiduciary duty of confidentiality owed to Plaintiff and member of the Class.

10. Accordingly, Plaintiff and the other Class Members seek redress against Defendant for breach of implied contract, breach of contract, invasion of privacy by the public disclosure of

private facts, common law negligence, negligent training and supervision, and breach of fiduciary duty of confidentiality.

11. Plaintiff, individually and on behalf of the other Class Members, seeks all (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds \$5 million, exclusive of interest and costs.

13. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conduct much of their business in this District and Defendant has caused harm to Class Members residing in this District

PARTIES

14. Plaintiff is an adult residing in Lee's Summit, Jackson County, Missouri.

15. Defendant DaVita, Inc. is, upon information and belief, a nationwide company with offices all through the country. They can be served through their registered agent at 1900 W Littleton Blvd., Littleton, Colorado 80120.

BACKGROUND FACTS

16. Certain allegations are made upon information and belief.

17. Defendant DaVita is a health care provider pursuant to state and federal law, providing health care and medical services to the general public, operating across the world, headquartered at 2000 16th St., JLD/SecGovFin, Denver, Colorado 80202.

18. As a part of its business operations, Defendant collects and maintains PHI and PII of its patients.

19. Plaintiff and the Class Members were patients of Defendant and, as a result, provided their PHI and PII to Defendant.

20. As such, Plaintiff and the Class Members entered into an implied contract with Defendant for the adequate protection of their PHI and PII.

21. Defendant is required to maintain the strictest privacy and confidentiality of Plaintiff and the proposed Class Members' medical records and other PHI and PII.

22. Defendant posts its privacy practices online, at <https://www.davita.com/privacy-practices>.

23. On April 14th, 2025, Defendant filed a Form 8-K with the United States Securities and Exchange Commission reporting a data security incident that impacted their PHI and PII.

24. According to the letter, “[o]n April 12, 2025, DaVita, Inc. (the “Company” or “we”) became aware of a ransomware incident that has encrypted elements of our network.”

25. The information that was contained in the files was undisclosed patient information.³

26. Ransomware group Interlock claimed that it was the group responsible for the attack, siphoning 20+ terabytes of data of DaVita patients.⁴

27. The disclosure of the PHI and PII at issue was a result of the Defendant's inadequate safety and security protocols governing PHI and PII.

28. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and the other Class Members' patient information.

³ *Id.*

⁴ *Id.*

29. Upon information and belief, the Breach affected tens of thousands of Defendant's patients.

30. As a direct and/or proximate result of Defendant's failure to properly safeguard and protect the PHI and PII of its patients, Plaintiff's and the other Class Members' PHI and PII was stolen, compromised and wrongfully disseminated without authorization.

31. Defendant had a duty to its patients to protect them from wrongful disclosures.

32. As a health care provider, Defendant is required to train and supervise its employees regarding the policies and procedures as well as the State and Federal laws for safeguarding patient information.

33. Defendant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

34. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH")⁵. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

35. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy Missouri. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

36. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

⁵ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

37. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

38. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

39. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

40. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

41. Under HIPAA:

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.⁶

42. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

43. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

44. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

45. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the

⁶ 45 C.F.R. § 160.103

confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” *See* US Department of Health & Human Services, Security Rule Guidance Material.⁷ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, “represent the industry standard for good business practices with respect to standards for securing e-PHI.” *See* US Department of Health & Human Services, Guidance on Risk Analysis.⁸

46. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

- (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
- (2) the recipient of the PHI;
- (3) whether the PHI was actually acquired or viewed; and
- (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."⁹

⁷ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>

⁸ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

⁹ 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

47. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

48. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

49. Defendant failed to provide proper notice to Plaintiff of the disclosure.

50. Defendant failed to conduct or improperly conducted the four-factor risk assessment following the unauthorized disclosure.

51. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their customers now have Plaintiff's and the other Class Members' compromised PHI and PII.

52. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendant's wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud¹⁰ and medical fraud.

53. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft, <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity->

¹⁰ According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

theft.html (last visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

54. The Federal Trade Commission correctly sets forth that “Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.” *Id.*

55. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver’s license or official identification card in the victim’s name but with their picture), using a victim’s name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim’s information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim’s name. Identity thieves also have been known to give a victim’s PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim’s name and an unwarranted criminal record.

56. According to the FTC, “the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data.”¹¹ Furthermore, “there is significant evidence demonstrating that technological advances and the ability to combine

¹¹ *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (<http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>).

disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.”¹²

57. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was \$354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

58. The unauthorized disclosure of a person’s Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064, October 2007, ICN 46327 (<http://www.ssa.gov/pubs/10064.html>). Thus, a person whose PHI and/or PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

59. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still

¹² *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report, 35-38 (Dec. 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

60. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-idtheft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

61. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and the other Class Members' prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

62. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the other Class Members' PHI and PII to unauthorized persons.

63. Upon information and belief, Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the

process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

64. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the other Class Members' PHI and PII to protect against anticipated threats to the security or integrity of such information. Defendant's unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

65. The actual harm and adverse effects to Plaintiff and the other Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's above wrongful actions and/or inaction and the resulting Breach requires Plaintiff and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiff and the other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

66. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiff and the other Class Members—typically spend hundreds of hours in

personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. See *Defend: Recover from Identity Theft*, <http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html>; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of \$1,513 and incur an average of \$354 of out-of-pocket expenses attempting to rectify the situation. *Id.* at 6.

67. Other statistical analyses are in accord. The GAO found that identity thieves use PHI and PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

68. Defendant's wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the other Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiff and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iii) out-of-pocket expenses to purchase credit monitoring,

internet monitoring, identity theft insurance and/or other Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach and (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not

CLASS ACTION ALLEGATIONS

69. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class, defined as follows:

Nationwide Class

All persons residing in the United States who are current or former customers of Defendant or any of Defendant's affiliate, parent, or subsidiary, and had their PHI and PII compromised as a result of the Data Breach.

In addition, Plaintiff brings this action on behalf of the following proposed Missouri Subclass, defined as follows:

Missouri Subclass

All persons residing in the State of Missouri who are current or former customers of Defendant or any of Defendant's affiliate, parent, or subsidiary, and had their PHI and PII compromised as a result of the Data Breach.

70. Both the proposed Nationwide Class and the proposed Missouri Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

71. Excluded from the proposed Class are any officer or director of Defendant any officer or director of any affiliate, parent, or subsidiary of Defendant; anyone employed by counsel in this action; and any judge to whom this case is assigned, her or her spouse, and members of the judge's staff.

72. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

73. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;
- b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;
- c. Whether Defendant owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PHI and PII;
- d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PHI and PII;
- e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PHI and PII in violation Section 5 of the FTC Act;
- g. Whether Plaintiff and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and
- h. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

74. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved.

Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

75. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PHI and PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct affected all Class Members in the same manner.

76. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

77. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

78. The preceding factual statements and allegations are incorporated herein by reference.

79. At all times relevant hereto, Defendant owed, and owe, a fiduciary duty to Plaintiff pursuant to Missouri common law, to keep Plaintiff's medical and other PHI and PII information confidential.

80. The fiduciary duty of privacy imposed by Missouri law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

81. Under their fiduciary duty, Defendant must institute safeguards to protect the privacy and security of their patients' medical records and medical information contained in those records.

82. Defendant breached their fiduciary duty to Plaintiff and the Class by disclosing Plaintiff's and the Class Members' PHI and PII to unauthorized third parties .

83. As a direct result of Defendant's breach of fiduciary duty of confidentiality and the disclosure of Plaintiff's and the Class Members' confidential medical information, Plaintiff suffered damages.

84. Defendant's wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Breach, Plaintiff and the Class have

incurred (and will continue to incur) damages in the form of, *inter alia*, (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII (iii) loss of privacy, (iv) humility, (v) embarrassment (vi) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

COUNT II
BREACH OF IMPLIED CONTRACT

85. The preceding factual statements and allegations are incorporated herein by reference.

86. Plaintiff and the other Class Members, as part of their agreement with Defendant, provided Defendant their PHI and PII.

87. In providing such PHI and PII, Plaintiff and the other Class Members entered into an implied contract with Defendant, whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class members' PHI and PII.

88. Under the implied contract, Defendant was obligated to not only safeguard the PHI and PII, but also to provide Plaintiff and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

89. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

90. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

91. Plaintiff and the other Class Members suffered and will continue to suffer damages

including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and Class members are entitled to nominal damages.

COUNT III **NEGLIGENCE**

92. The preceding factual statements and allegations are incorporated herein by reference.

93. Defendant owed, and continues to owe, a duty to Plaintiff and the other Class Members to safeguard and protect their PHI and PII.

94. Defendant breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PHI and PII.

95. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PHI and PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

96. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

97. Plaintiff's and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class members are entitled to nominal damages.

98. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law.

COUNT IV
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

99. The preceding factual statements and allegations are incorporated herein by reference.

100. Plaintiff's and the other Class Members' PHI and PII was (and continues to be) sensitive and personal private information.

101. By virtue of Defendant's failure to safeguard and protect Plaintiff's and the other Class Members' PHI and PII and the resulting Breach, Defendant wrongfully disseminated Plaintiff's and the other Class Members' PHI and PII to unauthorized persons.

102. Dissemination of Plaintiff's and the other Class Members' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is and will continue to be offensive to Plaintiff, the other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

103. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

104. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

105. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT V
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

106. The preceding factual statements and allegations are incorporated herein by reference.

107. At all times relevant hereto, Defendant owed, and owes, a fiduciary duty to Plaintiff and the proposed class pursuant to Missouri common law, to keep Plaintiff's medical and other PHI and PII information confidential.

108. The fiduciary duty of privacy imposed by Missouri law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity, health care provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.

109. Defendant breached its fiduciary duty to Plaintiff by disclosing Plaintiff and the other Class Members PHI and PII to unauthorized third parties.

110. As a direct result of Defendant's breach of fiduciary duty of confidentiality and the disclosure of Plaintiff's confidential medical information, Plaintiff and the proposed Class Members suffered damages.

111. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

112. Plaintiff and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

COUNT VI
VIOLATIONS OF MISSOURI MERCHANDISING PRACTICES ACT, MO. REV.
STAT. § 407.010 et seq.

113. The preceding factual statements and allegations are incorporated herein by reference.

114. RSMo. 407.020 prohibits the use of any “deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce”...

115. An “unfair practice” is defined by Missouri law, 15 CSR 60-8.020, as any practice which:

(A) Either-

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or
2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

116. An “unfair practice is defined by Missouri law,
15 CSR 60-8.020 (1)(B) provides that an “Unfair Practice in General” is

(1) An unfair practice is any practice which –

(A) Either –

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or
2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

15CSR 60-8.040 provides that an “Unfair Practice is:

An unfair practice for any person in connection with the advertisement or sale of merchandise to violate the duty of good faith in solicitation, negotiation and performance, or in any manner fail to act in good faith.

117. Plaintiff and Defendant are “persons” within the meaning of section 407.010 (5).

118. Merchandise is defined by the MMPA, to include the providing of “services” and, therefore, encompasses Healthcare services. Healthcare services are a good.

119. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

120. Maintenance of medical records are “merchandise” within the meaning of section 407.010(4).

121. Plaintiff’s and the Class’ goods and services purchased from Defendant were for “personal, family or household purposes” within the meaning of the Missouri Merchandising Practices Missouri Revised Statutes.

122. As set forth herein, Defendant’s acts, practices and conduct violate section 407.010(1) in that, among other things, Defendant has used and/or continues to use unfair practices, concealment, suppression and/or omission of material facts in connection with the advertising, marketing, and offering for sale of services associated with healthcare services. Such acts offend the public policy established by Missouri statute and constitute an “unfair practice” as that term is used in Missouri Revised Statute 407.020(1).

123. Defendant’s unfair, unlawful and deceptive acts, practices and conduct include: (1) representing to its patients that it will not disclose their sensitive personal health information to an

unauthorized third party or parties; (2) failing to implement security measures such as securing the records in a safe place; and (3) failing to train personnel.

124. Defendant's conduct also violates the enabling regulations for the MMPA because it: (1) offends public policy; (2) is unethical, oppressive and unscrupulous; (3) causes substantial injury to consumers; (4) it is not in good faith; (5) is unconscionable; and (6) is unlawful. *See* Mo Code Regs. Ann tit. 15, Section 60-8.

125. As a direct and proximate cause of Defendant's unfair and deceptive acts, Plaintiff and members of the Class have suffered damages in that they (1) paid more for medical record privacy protections than they otherwise would have, and (2) paid for medical record privacy protections that they did not receive. In this respect, Plaintiff and members of the Class have not received the benefit of the bargain and have suffered an ascertainable loss.

126. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

127. Plaintiff, on behalf of themselves and the Class, seek actual damages for all monies paid to Defendant in violation of the MMPA. In addition, Plaintiff seeks attorneys' fees.

COUNT VII
NEGLIGENT TRAINING AND SUPERVISION

128. The preceding factual statements and allegations are incorporated herein by reference.

129. At all times relevant hereto, Defendant owes a duty to Plaintiff and the Class to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their patients and their parents.

130. Defendant breached its duty to Plaintiff and the member of the Class by allowing its employees and agents to give access to patient medical records to an unauthorized user.

131. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

132. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

133. Defendant's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT VIII
NEGLIGENCE *PER SE*

134. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein

135. Plaintiff was under the medical care of the Defendant.

136. The Defendant is a covered entity for purposes of HIPAA.

137. Plaintiff is a member of the class HIPAA and HITECH were created to protect.

138. Plaintiff's private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

139. The Defendant gave protected medical information to an unauthorized third party or unauthorized third parties without the written consent or authorization of Plaintiff.

140. The Defendant gave protected medical information to unauthorized third parties without Plaintiff's oral consent or written authorization.

141. The information disclosed to an unauthorized third party or unauthorized third parties included private health information about medical treatment.

142. The Defendant's disclosure of the private health information of Plaintiff without consent or authorization is a violation of HIPAA and HITECH and is negligence *per se*.

143. Alternatively, Defendant violated HIPAA and HITECH in that it did not reasonably safeguard the private health information of Plaintiff from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

144. As a direct result of Defendant's negligence, Plaintiff and the Class Members suffered damages and injuries, including, without limitation, loss of the benefit of their bargain, a reduction in value of their private health information, loss of privacy, loss of medical expenses, loss of trust, loss of confidentiality, embarrassment, humiliation, emotional distress, and loss of enjoyment of life.

145. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

146. As a direct result of Defendant's negligence, Plaintiff have a significantly increased risk of being future victims of identity theft relative to what would be the case in the absence of the Defendant's wrongful acts.

147. As a direct result of Defendant's negligence, future monitoring, in the form of identity-theft or related identity protection is necessary in order to properly warn Plaintiff and the Class Members of, and/or protect Plaintiff and the Class Members from, being a victim of identity theft or other identity-related crimes.

148. Plaintiff, individually and on behalf of the Class, seek actual damages for all monies paid to Defendant in violation of the HIPAA and HITECH. In addition, Plaintiff seeks attorneys' fees.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Petition, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

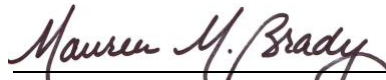
- A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representatives and appointing Plaintiff's counsel as Lead Counsel for the Class;
- B. Declaring that Defendant breached its implied contract with Plaintiff and Class Members;
- C. Declaring that Defendant negligently disclosed Plaintiff's and the Class Members PHI and PII;
- D. Declaring that Defendant has invaded Plaintiff's and Class Members' privacy;
- E. Declaring that Defendant breached its fiduciary duty to Plaintiff and the Class Members;
- F. Declaring that Defendant breached its implied contract with Plaintiff and the Class Members;
- G. Declaring that Defendant violated the Missouri Merchandising Practices Act;
- H. Declaring that Defendant was negligent by negligently training and supervising its employees and agents;
- I. Ordering Defendant to pay actual damages to Plaintiff and the Class Members;
- J. Ordering Defendant to properly disseminate individualized notice of the Breach to all Class Members;
- K. For an Order enjoining Defendant from continuing to engage in the unlawful business practices alleged herein;
- L. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff;
- M. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and
- N. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and the other Class Members, respectfully demands a trial by jury on all of her claims and causes of action so triable.

Date: May 1, 2025

Respectfully submitted,



Maureen M. Brady MO #57800

Lucy McShane MO#57957

MCSHANE & BRADY, LLC

4006 Central Street

Kansas City, MO 64111

Telephone: (816) 888-8010

Facsimile: (816) 332-6295

E-mail: mbrady@mcshanebradylaw.com

lmcshane@mcshanebradylaw.com

Counsel for Plaintiff and the Proposed Class